

Cisco FindIT Network Management常見問題

目標

Cisco FindIT Network Management是一個軟體，它允許您通過Web瀏覽器輕鬆管理整個網路（包括思科裝置）。它可以自動發現、監控和配置網路中所有受支援的思科裝置。此軟體還會向您傳送有關韌體更新的通知以及有關網路中不再受保修支援的裝置的資訊。

Cisco FindIT Network Management有兩個獨立的元件：一個稱為FindIT Network Manager的Manager和一個或多個稱為FindIT Network Probe的探測。

本文包含設定、配置和故障排除Cisco FindIT網路管理的常見問題及其答案。

常見問題

目錄

一般

1. [FindIT Network Management支援哪些語言？](#)

發現

2. FindIT [使用什麼協定來管理我的裝置？](#)
3. FindIT [如何發現我的網路？](#)
4. FindIT [是否進行網路掃描？](#)

連線埠管理

5. 為 [什麼連線埠管理不顯示堆疊連線埠？](#)

組態

6. [發現新裝置時會發生什麼情況？其配置是否會更改？](#)
7. [將裝置從一個裝置組移動到另一個裝置組時會發生什麼情況？](#)

安全注意事項

8. FindIT [網路管理器需要哪些埠範圍和協定？](#)
9. FindIT [網路探測需要哪些埠範圍和協定？](#)
10. [FindIT Network Manager和FindIT Network Probe之間的通訊安全程度如何？](#)
11. [FindIT是否對我的裝置具有「後門」訪問許可權？](#)
12. FindIT [中儲存憑據的安全性如何？](#)

13. [如何恢復管理GUI丟失的密碼？](#)

遠端存取

14. [從FindIT Network Management連線到裝置的管理GUI時，會話是否安全？](#)

15. [如何，當我開啟到另一裝置的遠端訪問會話時，與裝置的遠端訪問會話會立即註銷？](#)

16. [為什麼我的遠端訪問會話會失敗，錯誤如下：訪問錯誤：請求實體太大，HTTP標頭欄位是否超過支援的大小？](#)

軟體更新

17. [如何使Manager作業系統保持最新狀態？](#)

18. [如何在Manager上更新Java？](#)

19. [如何使探測作業系統保持最新？](#)

20. [什麼是Cisco FindIT Kaseya外掛？](#)

一般

1. [FindIT Network Management支援哪些語言？](#)

FindIT Network Management被翻譯成以下語言：

- 中文
- 英文
- 法文
- 德語
- 日語
- 西班牙文

發現

2. [FindIT使用什麼協定來管理我的裝置？](#)

FindIT使用各種協定來發現和管理網路。用於特定裝置的確切協定因裝置型別而異。這些協定包括：

- 多點傳送網域名稱系統(mDNS)和DNS服務探索 — 此通訊協定也稱為Bonjour。它查詢印表機、其它電腦以及這些裝置在本地網路上提供的服務等裝置。要瞭解有關mDNS的詳細資訊，請按一下[此處](#)。有關DNS服務發現的更多資訊，請按一下[此處](#)。
- Cisco Discovery Protocol(CDP) — 一種思科專有協定，用於共用有關其他直接連線的思科裝置的資訊，例如作業系統版本和IP地址。
- 鏈路層發現協定(LLDP) — 一種供應商中立協定，用於共用有關其他直連裝置 (如作業系統版本和IP地址) 的資訊。
- 簡易網路管理通訊協定(SNMP) — 網路管理通訊協定，用於在網際網路通訊協定(IP)網路上收集資訊和設定網路裝置，例如伺服器、印表機、集線器、交換機和路由器。
- RESTCONF — 網際網路工程任務組(IETF)草案，描述如何將Anyther Next

Generation(YANG)資料建模語言規範對映到RESTful介面。要瞭解更多資訊，請按一下[此處](#)。

[3. FindIT如何發現我的網路？](#)

FindIT Network Probe從偵聽CDP、LLDP和mDNS通告開始建立網路中裝置的初始清單。然後，探針使用支援的協定連線到每台裝置，並收集其他資訊，如CDP和LLDP鄰接表、媒體訪問控制(MAC)地址表和相關裝置清單。此資訊用於標識網路中的其他裝置，並重複此過程，直到發現所有裝置。

[4. FindIT是否執行網路掃描？](#)

FindIT不會主動掃描網路位址範圍。它結合了對某些網路協定的被動監控和主動查詢網路裝置的資訊。

連線埠管理

[5. 為什麼埠管理不顯示堆疊埠？](#)

埠管理圖是根據裝置通過管理協定提供的埠清單繪製的。處於堆疊模式時，堆疊連線埠會視為堆疊中的內部連線，因此裝置不會在管理通訊協定提供的清單中包含這些連線埠。

組態

[6. 發現新裝置後會發生什麼情況？其配置是否會更改？](#)

新裝置將新增到預設裝置組。如果已將配置檔案分配給預設裝置組，則該配置也將應用於新發現的裝置。

[7. 將裝置從一個裝置組移動到另一個裝置組時會發生什麼情況？](#)

與當前應用於原始裝置組但未應用於新裝置組的配置檔案相關聯的任何虛擬區域網(VLAN)或無線區域網(WLAN)配置將被刪除，並且與應用於新組且未應用於原始組的配置檔案相關聯的VLAN或WLAN配置將被新增到裝置中。系統配置設定將被應用到新組的配置檔案覆蓋。如果沒有為新組定義系統配置檔案，則裝置的系統配置將不會更改。

安全注意事項

[8. FindIT網路管理器需要哪些埠範圍和協定？](#)

下表包含FindIT網路管理器使用的協定和埠：

連接埠	方向	通訊協定	使用
TCP 22	傳入	SSH	通過命令列訪問Manager
TCP 80	傳入	HTTP	對Manager的Web訪問。重定向到安全Web伺服器（埠443）
TCP 443	傳入	HTTPS	對Manager進行安全Web訪問
TCP 1069	傳入	NETCONF/TLS	探測器和管理器之間的通訊
TCP 9443	傳入	HTTPS	遠端訪問探測GUI
TCP 50000-51000	傳入	裝置相關	遠端訪問裝置
UDP 53	出站	DNS	域名解析
UDP 123	出站	NTP	時間同步

UDP 5353	出站	mDNS	將多播DNS服務通告傳送到本地網路通告Manager
----------	----	------	----------------------------

9. FindIT網路探測需要哪些埠範圍和協定？

下表列出了FindIT網路探測所使用的協定和埠：

連接埠	方向	通訊協定	使用
TCP 22	傳入	SSH	通過命令列訪問探測
TCP 80	傳入	HTTP	對Manager的Web訪問。重定向到安全Web伺服器
TCP 443	傳入	HTTPS	對Manager進行安全Web訪問
UDP 5353	傳入	mDNS	來自本地網路的組播DNS服務通告。用於裝置
TCP 10000-10100	傳入	裝置相關	遠端訪問裝置
UDP 53	出站	DNS	域名解析
UDP 123	出站	NTP	時間同步
TCP 80	出站	HTTP	未啟用安全Web服務的裝置管理
UDP 161	出站	SNMP	網路裝置的管理
TCP 443	出站	HTTPS	啟用安全Web服務的裝置管理。訪問思科Web服務以獲取軟體更新、
TCP 1069	出站	NETCONF/TLS	探測器和管理器之間的通訊
UDP 5353	出站	mDNS	將多播DNS服務通告傳送到本地網路通告

10. FindIT Network Manager和FindIT Network Probe之間的通訊安全程度如何？

Manager和探測之間的所有通訊都使用傳輸層安全(TLS)1.2會話進行加密，該會話由客戶端和伺服器證書進行身份驗證。會話從探測到Manager啟動。首次建立管理器與探測之間的關聯時，使用者必須從探測登入到管理器，此時管理器和探測交換證書以驗證將來的通訊。

11. FindIT是否對我的裝置具有「後門」訪問許可權？

否。當FindIT發現受支援的思科裝置時，它將嘗試使用該裝置的出廠預設憑證訪問裝置，預設使用者名稱和密碼：cisco或預設的SNMP社群：公用。如果裝置配置已從預設配置更改，則使用者需要向FindIT提供正確的憑證。

12. FindIT中儲存憑據的安全性如何？

訪問FindIT的憑證使用SHA512演演算法不可逆地雜湊。裝置和其他服務(例如Cisco Active Advisor)的憑證將使用AES-128演演算法以可逆方式加密。

13.如何恢復丟失的管理GUI密碼？

如果丟失了管理GUI中所有管理員帳戶的密碼，則可以通過登入到探測或管理器的控制檯並運行**recoverpassword** 工具來重置密碼。此工具將思科帳戶的密碼重置為預設密碼cisco，或者，如果刪除了思科帳戶，它將使用預設密碼重新建立帳戶。以下是使用此工具重設密碼時提供的命令範例。

```
cisco@FindITProbe:~# recoverpassword
```

```
(y/n)y
```

```
cisco@FindITProbe:~#
```

遠端存取

[14.當我從FindIT網路管理連線到裝置的管理GUI時，會話是否安全？](#)

FindIT Network Management在裝置和使用者之間隧道遠端訪問會話。使用的協定將取決於終端裝置配置，但是FindIT將始終使用安全協定建立會話（例如，HTTPS將優先於HTTP）。如果使用者是通過Manager連線到裝置，則無論裝置上啟用了何種協定，會話都會在Manager和探測之間通過加密隧道。

[15.當我開啟到另一裝置的遠端訪問會話時，為什麼與裝置的遠端訪問會話立即註銷？](#)

當您通過FindIT Network Management訪問裝置時，瀏覽器將每個連線視為與同一個Web伺服器(FindIT)相連，因此將向其他所有裝置提供來自每個裝置的cookie。如果多個裝置使用相同的cookie名稱，則一個裝置cookie可能被另一個裝置覆蓋。最常見的情況是會話cookie，結果是cookie僅對最近訪問的裝置有效。使用同一cookie名稱的所有其它裝置都將看到cookie無效，並將註銷會話。

[16.為什麼遠端訪問會話會失敗，並出現以下錯誤：訪問錯誤：請求實體太大，HTTP標頭欄位是否超過支援的大小？](#)

使用不同的裝置執行多個遠端訪問會話後，瀏覽器將為探測域儲存大量cookie。要解決此問題，請使用瀏覽器控制元件清除域的cookie，然後重新載入頁面。

軟體更新

[17.如何使Manager作業系統保持最新？](#)

管理器將CentOS Linux發行版用於作業系統。包和核心可以使用標準CentOS過程更新。例如，要執行手動更新，請以cisco使用者身份登入到控制檯，然後輸入命令`sudo yum -y update`。系統不應升級到新的CentOS版本，並且除了思科提供的虛擬機器映像中所包括的程式包之外，不應安裝其他程式包。

[18.如何更新Manager上的Java？](#)

應從Oracle下載對Java的更新，然後使用以下命令手動安裝：

將新的Java包直接下載到Manager:

```
curl -L -O -H "Cookie:oraclelicense=accept-securebackup-cookie" -k  
http://download.oracle.com/otn-pub/java/jdk/<version>-<build>/jre-<version>-linux-x64.rpm
```

以下是範例：

```
curl -L -O -H "Cookie:oraclelicense=accept-securebackup-cookie" -k  
"http://download.oracle.com/otn-pub/java/jdk/8u102-b14/jre-8u102-linux-x64.rpm"
```

要安裝更新的Java版本，請執行以下操作：

步驟1.使用`sudo yum -y remove jre1.8.0_102`指令移除舊版本

步驟2.使用命令`sudo yum -y localinstall jre-<version>-linux-x64.rpm`安裝新版本

[19.如何使探測作業系統保持最新？](#)

該探測器對作業系統使用OpenWRT。可以使用`opkg`工具更新包含的包。例如，要更新系統上

的所有軟體包，請以cisco使用者身份登入控制檯並輸入命令update-packages。如有必要，思科將在新版本的探測中提供核心更新。除思科提供的虛擬機器映像中所包含的軟體包外，不應安裝其他軟體包。

[20. 什麼是Cisco FindIT Kaseya外掛？](#)

Cisco FindIT Kaseya外掛旨在通過將Cisco FindIT Network Manager與Kaseya Virtual System Administrator(VSA)緊密整合來提高運營效率。Cisco FindIT Kaseya外掛提供強大的功能，包括操作管理、控制面板、裝置發現、網路拓撲、遠端裝置管理、可操作警報和事件歷史記錄。

該外掛設計為極易安裝，只需點選幾下。它符合Kaseya本地VSA 9.3和9.4版的所有第三方整合要求。要瞭解更多資訊，請按一下[此處](#)。